PROCESS FOR MANAGING AN ELECTRONIC TRANSACTION BY CHIP CARD, TERMINAL AND CHIP CARD IMPLEMENTING THIS PROCESS

The present invention relates to electronic transactions carried out by means of a chip card.

It proposes a process for managing such an electronic transaction, as well as a terminal and a chip card implementing this process.

Customarily, during a transaction with a chip card, it is the reading terminal into which the chip card is inserted which manages the procedure for authenticating the card and the bearer thereof, as well as the procedure for validating the transaction.

In particular, the terminal of the reading terminal routinely requests the bearer of the card to indicate thereto his/her authentication code. Also, if the amount of the transaction exceeds a certain threshold, the reading terminal can decide to interrogate an external authorization center.

However, it is henceforth desired to be able to carry out very fast electronic transactions which can take place within very short times - for example less than 100 ms - and for which bearer authentication is not realizable.

Nowadays, fast electronic transactions are made possible by so-called "electronic purse" systems.

An electronic purse is a device which comprises a memory in which is stored a value corresponding to a monetary sum which is decremented as and when transactions are made by means of said purse.

However, electronic purses have drawbacks. In particular, they do not ensure the same security of transaction as bank cards. In particular, with an electronic purse it may happen that the latter registers a debit although the transaction at the level of the reading terminal is not taken into account.

An aim of the invention is to propose a process for managing an electronic transaction which makes it

possible to carry out transactions as speedily as with an electronic purse, but with security similar to that made possible by the currently known protocols for transactions by bank card.

The solution according to the invention consists of a process for managing an electronic transaction by means of a bank card of the microprocessor chip type and of a reading terminal able to talk to said card, in which the reading terminal sends a signal to said card which indicates thereto the amount of the transaction and in which said card compares this amount with a threshold transaction amount value and instigates a bearer authentication procedure when this amount is above said threshold, characterized in that, when this amount is below said threshold, said chip card compares with a threshold value the value of a counter, the so-called aggregate of small amounts counter, which value it increments by the value of the amount of the transaction and in that a procedure for authenticating the bearer of the card is instigated by said card as a function of the result of this comparison.

Thus, a card bearer benefits together with his bank card from a service which as far as he is concerned is akin to that of an electronic purse, but which is more secure, since it uses the existing infrastructure in respect of bank cards.

Furthermore, the traditional reloading function is eliminated therefrom, thereby conferring greater convenience on the use of the card.

This process is advantageously supplemented by the various following characteristics taken alone or according to all their technically possible combinations:

- the value of the counter is replaced with said incremented value when the value of the amount of the transaction is below the threshold transaction amount value;

- the value of the aggregate of small amounts counter is replaced with said incremented value when, as a function of the result of the comparison, the card bearer authentication procedure is not instigated by said card;
- when the card bearer's identification code has been verified, the card increments by the value of the amount of the transaction, the sum of the counter of small amounts and of a second counter, it compares the incremented sum with a threshold value and instigates the interrogation by the reading terminal of an authorization center as a function of the result of this comparison, said card resetting the two counters to zero when authorization is given by said center, the value of the second counter being replaced with the value of the incremented sum, if as a function of the result of the comparison, the card decides not to request the reading terminal to interrogate the authorization center, the value of the counter of small amounts then being reset to zero;
- the incrementation implemented by the chip card is a positive incrementation;
- the incrementation implemented by the chip card is a negative incrementation.

The invention also relates to a microprocessor chip card intended to be used to carry out electronic transactions, characterized in that it comprises means for implementing the aforesaid process.

Advantageously, this chip card comprises memory means for storing one or more threshold values and/or counter values, as well as means of comparison.

The invention also relates to a terminal for reading microprocessor chip cards, intended to be used to carry out electronic transactions, characterized in that it comprises means for implementing the aforesaid process.

Other characteristics and advantages of the invention will become further apparent from the description which follows of several modes of

implementation of the invention. This description is purely illustrative and nonlimiting. It must therefore be read in conjunction with the appended drawings in which:

- Figure 1 is a flow chart illustrating a possible mode of implementation in respect of the process proposed by the invention;
- Figure 2 is a flow chart illustrating another possible mode of implementation.

The various steps of the management processes illustrated in Figures 1 and 2 are implemented during an electronic transaction carried out by means of a bank type chip card.

This chip card comprises a microprocessor which is programmed in such a way as to implement a protocol which corresponds to these various steps, as well as ROM, EPROM, EEPROM or RAM memories in which are stored the various values calculated or taken into account during these various steps (amount of the transaction, values of counter(s), ceiling(s), etc.).

The reading terminal is programmed to implement the same process, the chip card and said terminal comprising means allowing them to talk to each other, these means possibly being of any type (bus using connection tracks carried by the chip card, exchanges via RF transmission/reception, etc.).

In Figure 1, the steps implemented by the chip card are depicted in the block referenced by C, those implemented by the reading terminal being depicted in the block referenced by L.

The transaction begins with an initialization of the chip card instigated by the reading terminal (step 1).

The card, in response, sends its identification to the reading terminal (step 2).

Next, the reading terminal requests the operator to input the amount M of the transaction (step 3). It sends this amount M to the card.

The latter implements a test 4 on the value of this amount M.

If this amount M is below a ceiling value VP1, the card increments a counter COMPT by the value of this amount M (step 5).

The card then compares the value of this counter COMPT with a threshold VP2, which may be different from the threshold VP1.

If the counter COMPT is below VP2, the microprocessor of the card calculates the signature ST of the transaction (step 7) and sends it to the reading terminal which verifies it and archives the amount of the transaction, as well as the details of the latter (steps 8 and 9).

If, conversely, the value of the counter COMPT is greater than VP2, the card requests the reading terminal for presentation of the bearer's code (step 10).

The bearer inputs his code (step 11).

The code is sent by the reading terminal to the card which verifies it (step 12).

After verification, the microprocessor of the card resumes the processing and calculates the transaction signature ST (step 7). Between the verification step 12 and the computation step 7, the counter COMPT is reset to zero. Thus, the counter COMPT is reset to zero after each positive verification of the confidential code (step 20).

The bearer's code is also requested by the card when the amount M is greater than the threshold value VP1 ("yes" response to test 4).

In this case, the bearer's code is verified and the amount M is not aggregated on the counter COMPT.

The conventional steps of a bank card transaction are run.

Optionally, or as a variant, provision may be made for the card to request the connection of the reading terminal to the banking system so as to obtain a transaction authorization therefrom.

With the transaction authorization, the reading terminal can, as a function of the information provided by the banking system, send the card an order to reupdate the ceilings VP1 and VP2.

As will have been understood, in the variant implementation just described with reference to Figure 1, the payment card aggregates on the internal counter COMPT the amount of the transactions which are below a certain threshold and requests authentication of the bearer only when the amount M is above this threshold or when the aggregated sum of the earlier transactions becomes greater than a given threshold.

As a variant, provision may be made for the counter COMPT to be reset to zero only under the supposition that the value of the counter COMPT is verified to be above the threshold value VP2 in step 6 and that the code input is recognized as being correct by the card.

Under this supposition, the counter COMPT is not reset to zero if, during step 4, the amount M is verified to be above the threshold value VP1.

It is reset to zero only if the amount M is below the threshold value VP1 and if in step 6 the counter COMPT is verified to be above VP2 and if the verified code is correct.

Thus, the counter COMPT is reset to zero only when on the one hand the sum of the small amounts reaches the threshold VP2 and on the other hand the bearer is authenticated by his code.

Again as a variant, the card can be used to carry out an incremental payment, for example in the case of a communication from a public telephone kiosk.

In this case, an increment loop is added between steps 7 and 3, and the signature ST is as a function of the sum incremented (ΣM) at the end of the communication, ΣM being reset to zero in the card on completion of the identification step 2.

Thus, at the end of the communication only a single transfer order ST is retained, containing the

sum of the charges levied; the user pays as a function of the duration of the communication and as and when the charges are levied.

Another variant implementation is illustrated in Figure 2.

This second variant consists in managing a second counter CPT2 in the card accumulating the aggregates performed on a first counter CPT1 of small amounts. If the value of the counter CPT2 reaches a second ceiling value VP2, defined by the bank and registered previously in the card, the card will demand the checking of a certificate calculated by an authorization center.

The procedure is as follows:

The card adds the amount M of the transaction to the value read from CPT1.

If (test 13) the sum CPT1+M reaches the ceiling value, VP1, the card demands the checking of the bearer's confidential code (steps 10, 11 and 12).

If the confidential code is correct, the card adds the value of CPT1+M to the value read from CPT2.

The new value obtained is compared with a threshold VP2 (test 14).

If the sum CPT1+M+CPT2 reaches the ceiling VP2, the card demands (step 15) the checking of a certificate computed by an authorization center interrogated by the terminal of the reading terminal L (step 16).

If the certificate is correct, the card resets the counters CPT1 and CPT2 to zero (step 17) and then computes and delivers the signature of the transaction (steps 7 et seq.).

If the certificate is incorrect, the card does not deliver the signature of the transaction and leaves the values of the counters CPT1 and CPT2 unaltered.

If the sum CPT1+M+CPT2 has not reached the ceiling value VP2, the card resets the counter CPT1 to zero and updates the counter CPT2 by replacing its previous value with CPT2+CPT1+M (step 18). Next it

computes and delivers the signature of the transaction (steps 7, 8 and 9).

If the confidential code is not correct, the card C does not deliver the signature of the transaction and leaves the counters CPT1 and CPT2 unaltered.

Sub A4 If the sum CPT1+M does not reach the ceiling value VP1, the card updates the counter CPT1 by replacing its previous value with the sum CPT1+M (step 19), and it then delivers the signature of the transaction (steps 7, 8 and 9).

Sub B6 The card just described can be used in postdebit mode. The amounts debited are aggregated, for example over 30 days at most, on the basis of bearer account number, and the bearer account is debited after the ceiling VP2 is exceeded or on completion of the 30 days of the value of the amounts aggregated since the last debit of the account. The amounts can be aggregated:

- on the collection server after collection of the transactions stored on the trading terminals. In this case, the exceeding of the ceiling VP2 triggers in the card via the terminal a request for authorization of amount equal to the new ceiling VP2 which can be redefined by the bank.
- In the card itself. In this case, the exceeding of the ceiling VP2 triggers in the card via the terminal a resetting of the aggregate and an authorization request. In this case it is necessary to have the customer pay a deposit when obtaining his card, to prevent the "deliberate" theft or loss of his card (thus avoiding the debiting of the aggregate. This deposit can be disguised, that is to say included within the annual subscription of the card.

The card can also be used in predebit mode. In this case, the value VP1, and for the variant of Figure

2, the value VP2, is (or are) prepaid by the bearer and updated in the card, with the aid of the certificate received which is dependent on the amount prepaid by the user.

If the user should find himself on a terminal with no identification keypad or which is not connected to a telecommunication network, and should the prepaid value VP1, VP2 be reached, he will have to get onto a device of the bank (automatic teller machine - voucher dispenser or public telephone) so that the operations for checking the certificate issued by the authorization center can be carried out. The transaction in this case being fictitious, no amount being debited from the customer's account, except in the predebit application.

Again as a variant, the card need not utilize the bearer authentication code.

In this case, the comparison of the amount of the transaction with the threshold VP1 is not carried out and VP1 is not used. When the value COMPT stored in the card is greater than or equal to the threshold VP2, the card does not deliver the transaction signature ST.

A tolerance on VP2 is defined so as to accept the values of COMPT which are slightly greater than VP2 and thus allow the overstepping by COMPT of the value VP2 which disables the card.

The card can be discardable, when VP2 is reached, the card is no longer usable. However, in particular if the card is refundable, the bearer can return the card to the bank which with the aid of a secure procedure resets the value of COMPT to zero, before reintroducing it into a new usage cycle.

Or else, the card can be enabled by the bank with the aid of a secure on-line procedure. In the course of this procedure the bearer is authenticated, for example, with the aid of a second payment card or a code verified by the server of the bank, and COMPT is reset to zero after verification by the card of a certificate computed by the bank.

Sub A5

In the examples above, the counters CPT1 and CPT2 are incremented from the value 0 to a ceiling value. It is also possible to count downwards, the counters being initialized to the ceiling value VP1 and VP2 and then decremented down to the value 0, the counting can also be done on negative values etc.

As will have been understood, with the management process proposed by the invention, the aggregated amount is compared, not with an amount previously reloaded into the card, but with a maximum value fixed as a function of the risk which the issuer of the card is prepared to take. This comparison is a means of limiting the customer's expenses over time, and this is one of the roles of the card, in addition to authentication. The maximum value chosen can be regarded as a kind of permanent credit granted to solvent customers, the bank being remunerated for example by virtue of a commission on transactions.

The small transactions are submitted:

- either individually by the trader, like normal-amount transactions, using the banking infrastructure. The only function of the customer aggregate in the card is then to limit the customer's expenses (moderator role);
- or with a trader aggregating option, which assumes that the customer aggregate is also submitted (by the card, in the course of a transaction) to the bank for invoicing. This option obviously does not allow the same checks as the first.

A management of credit in the card can be as follows:

- to be valid a transaction must be signed by the card. The signature ST1, printed on the customer slip, serves to resolve any disputes.
- The data of a transaction are stored in the terminal's submission file and then collected once a day by the trader's bank collection center. The transactions of small amounts are sent to the bearer's bank and are not processed individually by the latter: they are stored to allow the auditing of the system, to

resolve any disputes and to settle with the trading bank.

- The trader's bank account is credited in accordance with the aggregate of the small amounts collected in the terminal daily.

- The amount of a transaction is aggregated in the credit counter of the card. The card verifies the value of the credit counter and the duration of the credit.

Examples of transactions processed by the card are given in the following tables.

Table I/

The credit counter of the card has reached the ceiling value fixed by the bank. The data of the table are managed in the card. The date of the transaction, the amount of the transaction are provided to the card by the terminal.

Transaction number	Amount of the transaction	Counter of credits	Date of the transaction	Ceiling fixed by the bank	Maximum duration of the credit
1	10	10	02/08/1999	100	1 month
2	20	30	03/08/1999	100	
3	40	70	05/08/1999	100	
4	20	90	05/08/1999	100	
5	30	120	07/08/1999	100	
		0			

Table II/

The maximum duration of credit of the card is reached.

Transaction number	Amount of the transac-tion	Counter of credits	Date of the transaction	Ceiling fixed by the bank	Maximum duration of the credit
1	10	10	02/08/1999	100	1 month
2	20	30	10/08/1999	100	

3	15	45	15/08/1999	100	
4	20	65	25/08/1999	100	
5	0	70	03/09/1999	100	
		0			

The transaction process proposed by the invention has numerous advantages:

- the security is that of the bank card since the debits are verified a posteriori by the bearer, the trader and the bank;
- the payment with debit/credit card can be made on a contactless card since there is no longer any routine inputting of the confidential code and moreover, should the contactless exchanges be interrupted, the transaction can easily be canceled;
- the bank card network is not modified and there is the possibility of reusing the server for accumulating the amounts of payphone transactions over a month by bank card;
- it is no longer possible to deceive the terminal regarding the response to the verification of the bearer code, since the transaction will only be continued if the bearer code is correct.